sogei

SERVIZIO DI COOPERAZIONE INFORMATICA PER SERVIZIO BOOLEANO DI RISCONTRO CORRISPONDENZA SOGGETTO GIURIDICO – RAPPRESENTANTE LEGALE SPECIFICHE TECNICHE- CORNICE DI SICUREZZA

Compilato : E. Minazzato

Rivisto :

Approvato :

Versione : 1.0

INDICE

1. MODALITÀ DI ACCESSO AI SERVIZI

A seguito del Provvedimento emesso dall' Autorità Garante il 18 settembre 2008 per la protezione dei dati personali (e successive integrazioni di marzo 2010 - sezione "Specifiche tecniche della nuova classe di web-services") inerente l'erogazione di web-services da parte dell'Agenzia Entrate, è stata predisposta una infrastruttura di erogazione dei servizi integrata da una "Cornice di sicurezza", per ottemperare alle misure previste.

1.1 L'INFRASTRUTTURA DI ACCESSO

L'infrastruttura predisposta consente di utilizzare il servizio con accesso da rete SPC, all'interno di un sistema di Identità Federata, nel quale l'Agenzia Entrate rappresenta il fornitore del servizio (Service Provider SP) mentre l'Ente fruitore del servizio stesso, assume il ruolo di fornitore di identità (Identity Provider IdP).

L'Ente che intende partecipare all'Identità Federata, dovrà sottoscrivere un accordo di trust, nel quale saranno specificate le politiche di sicurezza che l'Ente si impegna a rispettare al proprio interno (ad esempio le password policy applicate dall'Ente nel proprio sistema per le credenziali degli utenti).

Gli utenti dell'Ente Identity Provider, potranno accedere ai servizi esposti dall'Agenzia mediante l'utilizzo di applicazioni dell'Ente stesso, autenticandosi presso il proprio sistema con le credenziali da questo rilasciate.

Al successivo paragrafo 2 sono riportati i dettagli tecnici inerenti l'accesso ai servizi.

1.2 TRACCIAMENTO DELLE OPERAZIONI

L'Autorità Garante, sempre nel provvedimento marzo 2010, precisa che il sistema di tracciamento dell'Ente Service Provider, oltre a registrare le informazioni rese disponibili dal servizio erogato, acquisisca anche le informazioni ricevute mediante l'asserzione SAML.

Pertanto, per ottemperare alle prescrizioni del garante, sono stati integrati nel tracciamento degli accessi effettuati mediante utilizzo dei Web Services, i seguenti dati:

- Ente connesso, desunto dal NameID presente nell'asserzione SAML

- Utente remoto dell'Ente (User), desunto dall'attributo dell'asserzione SAML

Indirizzo IP della postazione dell'utente connesso, desunta dall'attributo dell'asserzione SAML (IP-User).

2. ACCESSO AI SERVIZI – DETTAGLI TECNICI

In conformità alle direttive del Garante della privacy l'accesso ai web services dell'Agenzia delle Entrate dovrà avvenire in un sistema di identità federata basato sul protocollo standard SAML 2.0.

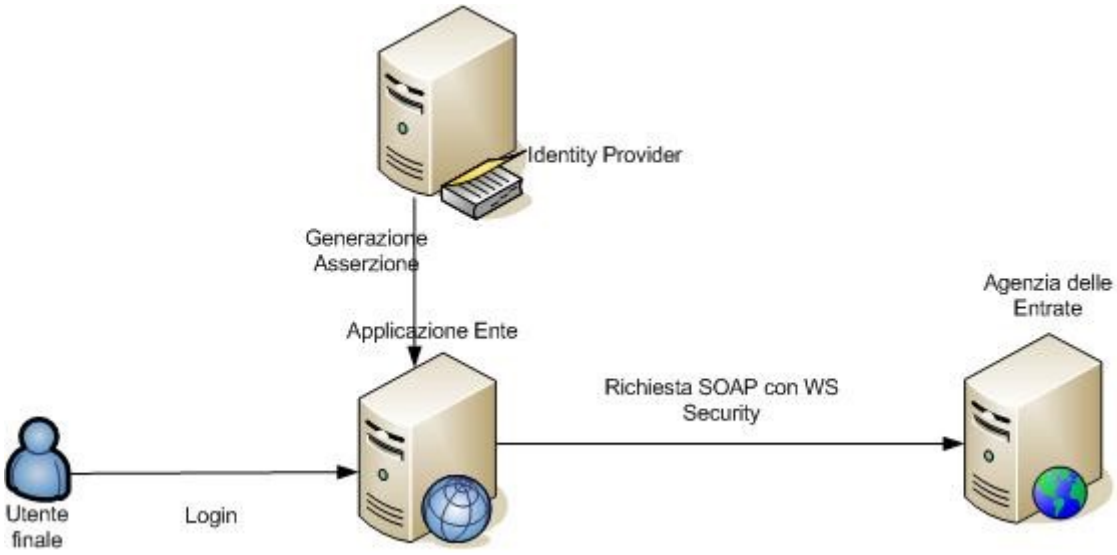
Questo documento descrive le modalità tecniche di interazione tra le applicazioni web services dell'Agenzia delle Entrate ed i sistemi dell'ente esterno.

In questo scenario si utilizzeranno gli standard della WS-Security ed in particolare il SAMLTokenProfile, che prevede, per la fase di autenticazione/autorizzazione dell'utente, l'utilizzo dello standard di federazione SAML. In particolare, in questo specifico caso, l'Agenzia rappresenta, all'interno di un sistema di Identità Federata, il fornitore del servizio (Service Provider SP) mentre gli altri enti svolgono il ruolo di fornitori di identità (Identity Provider IdP).

In particolare nella fase di autenticazione l'asserzione SAML dovrà contenere l'identificativo dell'ente, l'identificativo dell'utente finale (ovvero l'utenza utilizzata per l'autenticazione sul sistema dell'Ente) che ha originato la richiesta del web services e l'indirizzo ip della postazione dal quale questo utente opera.

L'applicazione chiamante dell'Ente dovrà raccogliere le informazioni sopra specificate ed inserirle nei formati di seguito descritti in un asserzione SAML 2.0 all'interno del WS Security header.

Il flusso è rappresentato nella seguente figura:



L'utente si autentica sul proprio Identity Provider che rilascia, per lo stesso, un'asserzione SAML. Tale asserzione viene inserita nel WS-Security Header della SOAPRequest inviata al sistema dell'Agenzia.

La procedura di autenticazione dell'utente deve essere protetta dal rischio di intercettazione delle credenziali da meccanismi crittografici di robustezza almeno equivalente a quella offerta dal protocollo TLS v1.2 esclusivo, chiavi RSA 2048 bit e cifrari basati su algoritmo AES.

Il server dell'Agenzia riceve la richiesta, verifica la validità dell'asserzione contenuta nel WS-Security Header della SOAPRequest, controllando la correttezza della firma digitale apposta, e, in caso positivo, concede l'accesso al servizio richiesto.

L'asserzione SAML conterrà come utenza l'identificativo dell'Ente Identity Provider, mentre l'identificativo dell'utente autenticato e altre informazioni utili per il tracciamento degli accessi, sono contenute negli attributi dell'asserzione stessa. Di seguito un maggior dettaglio di quanto descritto sopra.

2.1 FASE DI AUTENTICAZIONE/AUTORIZZAZIONE, MEDIANTE L'UTILIZZO DELLO STANDARD DI FEDERAZIONE SAML

L"utente dell'Ente si autentica sul proprio sistema che rilascia, per lo stesso, una asserzione SAML che viene firmata dall'Ente, inserita nel WS-Security Header della SOAPRequest e inviata al sistema dell'Agenzia a testimonianza dell'avvenuta autenticazione. L'asserzione SAML, dovrà contenere i campi di seguito descritti:

nome campo	**Descrizione**
NameID	Deve essere valorizzato con l'identificavo associato all'IDP che accede al sistema. Nel caso specifico, deve contenere il codice fiscale del soggetto che è stato autorizzato all'accesso seguito da un codice di tre cifre identificativo dell'ufficio attribuito all'utente. Il formato è il seguente: <codice fiscale/codUff> Esempio: 01234567890/XXX Nell'esempio SAML riportato nel documento ***CodiceEnte***
User	Deve essere valorizzato con l'identificavo univoco associato dall'IDP all'utente autenticato (Persona Fisica) che effettua le richieste. Ad esempio un codice fiscale

	di persona fisica o altro. La lunghezza dell'identificativo inserito non deve superare i 16 caratteri. Nell'esempio SAML riportato nel documento ***Useridutentefinale***
IP-User	Deve essere valorizzato con l'indirizzo IP della postazione client assegnata nell'ambito dell'IDP all'utente (User) Nell'esempio SAML riportato nel documento ***Indirizzoippostazioneutente***

L'intervallo di validità dell'asserzione SAML, generata nel contesto dei sistemi dell'Ente fruitore, non deve essere superiore ai 10 minuti; tale prescrizione si concretizza nella congrua valorizzazione dell'attributo NotOnOrAfter dell'elemento <SubjectConfirmationData> presente nell'asserzione stessa.

2.2 ESEMPIO DI RICHIESTA SOAP

Si riporta di seguito a titolo di esempio il formato della richiesta SOAP di un servizio generico:

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:test="http://test.it.finanze.sogei">
<soapenv:Header>
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-wssecurity-secext-1.0.xsd">
<saml2:Assertion Version="2.0" ID="ID0f7b725d-c07b-4dc7- 914c-
2aec43db6655" IssueInstant="2009-08-03T09:01:43Z"
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
xmlns:SOAP="http://schemas.xmlsoap.org/soap/envelope/">
<saml2:Issuer>Datapower20IDP</saml2:Issuer>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
<SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#ID0f7b725d-c07b-4dc7-914c-2aec43db6655">
<Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
signature"/>
<Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</Transforms>
<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<DigestValue>60MvNFhK81il++KWKL7/9Rnjwjk=</DigestValue>
</Reference>
```

```
</SignedInfo>
<SignatureValue>D784DonwGHlq017dCQry9kSpIDqSDF4IoEFxCC0J2D3eKksp1Y/EPPeNw
MCrd5oBbRYpluywJ0UGUSyyVFH9hXtNRDcXW/Ayy9iIFU7zSLdYKBfIJ4GCvJS983icqXbkHK
VA+KZBCS/gL5cTmMQay8=</SignatureValue>
<KeyInfo>
<X509Data>
      <X509Certificate>MIIDpzCCAo+gAwIBAgIQIkQhhMstoeFiAjccw5IQKTANBgkqh
kiG9w0BAQUFADBjMdlaS5pdDELMAkGA1UEBhMCSVQxDjAMBgNVBAoVpMQ8wDQYDVQQLEwZDQ0
9JVFQxETAPBgNVBAMTCGNhY2NvaXR0MB4XDTA3MDEzMDUwNVowPjELMAkGA1UEBhMCSVQxDjA
MBgNVBAoMBVNvZ
VpMRAwDgYDVQQLDAdTSVMtSVRBMQ0wCwYDVQQDDAR4aTUwMIGfMA0GCSqGSIb3DQEBAQGNADC
BiQKBgQCrhEEUbV57ec/MLkFoag1k4XPIK6JpeD/Zq9D/XpI42vo6nR/FL5l7KuV//RXAyEoK
fo3YgvRCSAq0tIGe1T5B4JjeiHcE3bJ7n3iJLkX2iNohNHcHNc8o8W1H9TQ5QSYmfW6dhvh2l
Kz3t1sOVHMisQ+UED6gEsXcCwIDAQABo4H/MIH8MB8GA1UdIwQYMBaAFA+ut542L0/lq/96yr
/E+H9MA4GA1UdDwEB/wQEAwIDuDARBglghkgBhvhCAQEEBAMCBkAwJQYDVR0RBB4wHIIaeMC5
hcmNoaXRldHR1cmEuc29nZWkuaXQwHQYDVR0OBBYEFJZWYX5NLPZC6N68aAUfIMT/asUdHwQt
MCswKaAnoCWGI2h0dHA6Ly9jbS1lbnRyYXRlMjo0NDcvY2FjY29pdHQuY3JsMDUdLgQzMDEwL
6AtoCuGKWh0dHA6Ly9jbS1lbnRyYXRlMjo0NDcvY2FjY29pdHRfZGVsdGEuY3JGCSqGSIb3DQ
EBBQUAA4IBAQAOP5LDLLHhRVKaUs5Pffz62i3VOQUtNTnB4UvLLhXlt6WapUT8JUluKWNThn0
C85+ZeJ/YKNFTclMErnhGJA/XtDvOgrnS1rARnZAQ4KQDj5sn4lnhVlhfvFFOipebgH025Bfi
huAWRDa1lg4apZrhprF479IQ54fFafLhr6BjWG0uAxaIT8Nze0UCgCF+BwVlOCWoM1kklLVnv
VAuB0JREE1JZO1GLG/1fHofsa5McLejq6LTXNyef8OC310F8fk+XDeYpk4+IeZn6PFnL1Udvv
cAtHnwd
</X509Certificate>
<X509IssuerSerial>
<X509IssuerName>CN=caccoitt, OU=CCOITT, O=Sogei,
C=IT,=sluciani@sogei.it</X509IssuerName>
      <X509SerialNumber>455475078835825034596852000308835164 57</X509Seri
alNumber>
</X509IssuerSerial>
</X509Data>
</KeyInfo>
</Signature>
<saml2:Subject>
<saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameidformat:
unspecified">CodiceEnte 1</saml2:NameID>
<saml2:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml2:SubjectConfirmationData NotBefore="2009-08-03T08:51:43Z"
NotOnOrAfter="2009-08- 03T17:31:43Z"/>
</saml2:SubjectConfirmation>
</saml2:Subject>
<saml2:Conditions NotBefore="2009-08-03T08:51:43Z" NotOnOrAfter="2009-08-
03T17:31:43Z"/>
<saml2:AuthnStatement AuthnInstant="2009-08-03T09:01:43Z"
SessionNotOnOrAfter="2009-08- 03T17:31:43Z">
<saml2:AuthnContext>
      <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes
:unspecified</saml2:AuthnContextClassRef>
</saml2:AuthnContext>
</saml2:AuthnStatement>
```

```
<saml2:AttributeStatement>
<saml2:Attribute Name="User"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml2:AttributeValue>Useridutentefinale 2</saml2:AttributeValue>
</saml2:Attribute>
<saml2:Attribute Name="IP-User"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml2:AttributeValue>Indirizzoippostazioneutente
3</saml2:AttributeValue>
</saml2:Attribute>
</saml2:AttributeStatement>
</saml2:Assertion>
</wsse:Security>
</soapenv:Header>
<soapenv:Body>
<test:interrogazioneEsempio>
<test:codiceFiscale>lcwesr74c02h844s</test:codiceFiscale>
</test:interrogazioneEsempio>
</soapenv:Body>
</soapenv:Envelope>
```